UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA v. TIMOTHY LIVINGSTON, a/k/a "Mark Loyd"	Criminal No. 15-626 (WJM) **EXPERT DECLARATION OF DR. MATTHEW J. EDMAN** **October 20, 2016**

EXPERT DECLARATION OF DR. MATTHEW J. EDMAN

I, Matthew J. Edman, make the following expert declarations in connection with the above-referenced matter.

I. BACKGROUND AND QUALIFICATIONS

1. I am over the age of eighteen (18) and not a party to this action. The following facts are based upon my own personal knowledge, education, and experience. If called as a witness, I could and would testify to the truth of the declared facts under oath.

2. I am currently employed as a Director in Berkeley Research Group, LLC's ("BRG") Global Cyber Security & Investigations practice. I regularly provide expert consultation to clients, including corporations and government agencies, regarding computer and network security best-practices, as well as conduct cyber incident response and investigative analysis.

3. From 2014 to 2015, I was employed as a Senior Director in FTI Consulting, Inc.'s Global Risk and Investigations Practice in the Cyber Security & Investigations Group. I worked on numerous matters related to computer and network security, including conducting penetration testing and vulnerability assessments for multiple clients, and performing forensic evidence collection and analysis in response to potential breaches of client systems and networks.

4. From 2013 to 2014, I was employed as a Senior Vulnerability Engineer by Bloomberg, LP, a global financial services, software, and media company. As a member of the firm's Vulnerability Analysis Team, my professional responsibilities focused on the protection of sensitive client data from both internal and external threats through continuous vulnerability research and penetration testing of the firm's network infrastructure, websites, software, and mobile applications. I was also involved in software and network architecture design reviews and risk assessments for numerous business areas across the company.

5. From 2009 to 2013, I was employed as a Lead Cyber Security Engineer by The MITRE Corporation, a federally funded research and development center, where I specialized in computer and network security research and development related to systems for anonymous communication on the Internet.

6. From 2007 to 2009, I was a software developer for The Tor Project, Inc. ("The Tor Project"). The Tor Project is a nonprofit research and education organization that develops software to help users protect their privacy on the Internet.

7. I have authored or co-authored multiple research papers in peer-reviewed conferences and journals related to novel techniques for cryptographic security and authentication in wireless networks, and the design, implementation, and analysis of anonymous communication systems on the Internet, including:

a. Matthew Edman, Aggelos Kiayias, Qiang Tang, Bulent Yener. *On the Security of Key Extraction from Measuring Physical Quantities.* In IEEE Transactions on Information Forensics and Security 11(8), August 2016.

b. Matthew Edman, Aggelos Kiayias, Bulent Yener. *On Passive Inference Attacks Against Physical Layer Key Extraction*. In Proceedings of the 2011 European Workshop on System Security (EuroSec '11), April 10, 2011, Salzburg, Austria.

c. Matthew Edman, Bulent Yener. *On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems*. In ACM Computing Surveys 42(1), January 2010.

d. Matthew Edman, Paul Syverson. *AS-awareness in Tor Path Selection*. In Proceedings of the 2009 ACM Conference on Computer and Communications Security (CCS '09), November 9-13, 2009, Chicago, IL.

e. Matthew Edman, Justin Hipple. *Vidalia: Towards a Usable Tor GUI*. In Proceedings of the 2007 Symposium on Usable Privacy and Security (SOUPS '07), July 18-20, 2007, Pittsburgh, PA.

f. Matthew Edman, Fikret Sivrikaya, Bulent Yener. *A Combinatorial Approach to Measuring Anonymity*. In Proceedings of the 2007 IEEE International Conference on Intelligence and Security Informatics (ISI '07), May 23-24, 2007, New Brunswick, NJ.

8. From 2007 to 2009, I served as an invited member of the technical program committee for the Association for Computing Machinery's Conference on Computer and Communications

Security. I have also served as an invited member of the technical program committee for the International Financial Cryptography Association's 2009 International Conference on Financial Cryptography and Data Security. Additionally, I have served as an external reviewer for several academic conferences and journals, including The Institution of Engineering and Technology's Information Security Journal and the Privacy Enhancing Technologies Symposium.

9. I received a B.S. in Computer Science from Baylor University in 2005, a M.S. in Computer Science from Rensselaer Polytechnic Institute in 2007, and a Ph.D. in Computer Science from Rensselaer Polytechnic Institute in 2011.

10. I have previously filed an expert report and testified as an expert in a deposition and at trial in the matter of *Spanski Enterprises, Inc. v. Telewizja Polska, S.A.,* Case No. 12-CV-957 (TSC) in the United States District Court for the District of Columbia. I have been retained as an expert in other matters that were settled prior to the submission of expert reports or testimony. A true and correct copy of my CV is attached to this declaration as Appendix A.

II. **SCOPE OF DECLARATION**

11. I have been retained as an expert in the above-captioned case by counsel on behalf of Defendant, Timothy Livingston a/k/a "Mark Loyd", to provide my analysis and opinions, based on my education and experience, as well as my review of the materials described in this report, on the following subjects:

a. review the contents of Government's Trial Exhibit 4001 and, to the extent possible, determine the overall nature and structure of its contents and any relevant computer search terms that may have been used to compile, group, and/or filter the set of data included in Trial Exhibit 4001;

b. review Exhibits 4 – 10 from the October 20, 2016 declaration of Mr. Ansel Halliburton and determine, to the extent possible, whether they appear to me to be an accurate rendering of the emails and/or email attachments to which they purportedly correspond;

c. review the contents of the files “uce.2015111012.020599.eml” and “uce.2016042418.028286.eml” from Trial Exhibit 4001 and determine, to the extent possible, whether they appear to me to be related to either [redacted] (Corporate Victim #2) or [redacted] (Corporate Victim #1); and

d. review the contents of the file “uce.2013070803.011501” from Trial Exhibit 4001 and determine, to the extent possible, whether it appears to represent an email submitted to the FTC by an individual person or by an automated software program.

12. In forming the opinions described in this report, I have reviewed the following documents and other materials previously produced in this matter:

a. Government’s Exhibit List in the matter of United States of America v. Timothy Livingston (Updated September 13, 2016);

b. Trial Exhibit 4001 which is described in Government’s Exhibit List as “FTC Search Data” and was provided to me by counsel for Defendant on October 10, 2016; and

c. Exhibits 4 – 10 from the October 20, 2016 declaration of Mr. Halliburton and provided to me by Mr. Halliburton on October 20, 2016.

13. I reserve the right to supplement or amend my opinions in light of additional evidence, testimony, or information that may be provided to me after the date of this declaration. I also

reserve the right to supplement or amend my opinions in response to any further expert declarations or reports. I expect that I may be called as a witness. If that occurs, I may produce or assist in producing exhibits for trial based on the documentation attached to or described in this declaration, its exhibits, or any supplemental reports and exhibits.

14. BRG is being paid $660 per hour for my work in this matter, excluding any potential deposition or trial testimony which is billed at a rate of $750 per hour. My compensation is not contingent on the outcome or resolution of this or any other legal matter.

ANALYSIS & OPINIONS

A. The complete methodology used to compile, group, and/or filter the set of data included in Trial Exhibit 4001 is not immediately apparent nor is it well documented.

15. The contents of Trial Exhibit 4001 were provided to me on October 10, 2016 by Mr. Halliburton, counsel for Defendant. Trial Exhibit 4001 as provided to me included one ".zip"[1] archive file named "Batch Search Results.zip", which consisted of a folder named "Initial Result Set" containing approximately 40,000 files representing emails and email attachments whose recipients included "spam@uce.gov." Trial Exhibit 4001 also included four top-level folders containing additional subfolders and files representing emails and email attachments. The top-level folders were named as follows:

Folder Name	# of Files
[redacted].2 March-April 2013	33
[redacted].2 March-April 2013 (No Duplicates)	22
[redacted].2-14 IP Range	774
[redacted].2-14 IP Range (No Duplicates)	372

16. Trial Exhibit 4001 does not include any documentation describing the methodology used to collect and validate the set of files contained within the Exhibit, nor did it contain

[1] ZIP is a compression format that compresses multiple individual files and stores the results within a single archive file. A ZIP archive file typically ends in the file extension ".zip".

documentation describing specifically the methodology used to filter and sort files into the folders described above. Trial Exhibit 4001 does include a README.txt file stating that "[t]he files in in the ZIP are .eml files"[2] and advises readers to use a text-based application (e.g. Microsoft Notepad) to review the files rather than a graphical email reader (e.g. Microsoft Outlook).

17. Based on a review of the top-level folders, their subfolders, and .eml file contents, I inferred that emails contained within the folders "[redacted].2 March-April 2013" and "[redacted].2 March-April 2013 (No Duplicates)" were intended to contain emails and email attachments sent between March and April 2013 that meet one or more of the following criteria:

a. the string "240[redacted]" appeared at least once within an email file or one of its attachments;

b. the string "240[redacted]" appeared at least once within an email file or one of its attachments;

c. the string "[redacted]" appeared at least once within an email file or one of its attachments; or

d. the IP address [redacted].2 appeared at least once within an email file or one of its attachments.

18. According to publicly available WHOIS information, the IP address [redacted].2 is managed by [redacted] (Corporate Victim #2) and is associated with the domain name "[redacted].com."

19. Despite the implied search terms, some of the emails contained within the folders "[redacted].2 March-April 2013" and "[redacted].2 March-April 2013 (No Duplicates)" include

[2] ".eml" is a file extension typically associated with email files.

emails and/or email attachments that meet none of the criteria described above (i.e. the results likely include false positives). For example, the file "uce.2013033112.030329.eml" includes one email attachment containing the search terms listed above, but also includes 28 other email attachments that match none of the search terms nor any other readily identifiable pattern.

20. I inferred that the top-level folders "[redacted].2-14 IP Range" and "[redacted].2-14 IP Range (No Duplicates)" were intended to include emails and email attachments that contain IP addresses in the range of [redacted].2 through [redacted].14 one or more times. According to publicly available WHOIS information, the IP addresses within this range are managed by [redacted] and associated with the domain "[redacted].com.br."

21. Again, however, the files within these two top-level folders include many emails or email attachments that do not reference an IP address within the range described in the top-level folder names. For example, the file "uce.2015102320.045637.eml" contains one email attachment containing the IP address [redacted].13, but also contains 49 other email attachments that are unrelated to (a) the IP address [redacted].13, (b) any IP address within the range [redacted].2 through [redacted].14, (c) the domain "[redacted].com.br", or (d) any of the search terms previously described above related to [redacted], [redacted] (Corporate Victim #2), and associated keywords.

B. **Exhibits 4 – 10 from the October 20, 2016 declaration of Mr. Ansel Halliburton appear to be accurate renderings of the emails and/or email attachments to which they correspond.**

22. The contents of Exhibits 4 – 10 from the October 20, 2016 declaration of Mr. Ansel Halliburton were provided to me on October 20, 2016 by Mr. Halliburton as a series of PDF files purportedly depicting a graphical rendering of selected emails and email attachments from Trial Exhibit 4001.

23. I reviewed Halliburton Exhibit 4, which was represented to me as a graphical rendering of the contents of the file “uce.2016042418.028286.eml” from Trial Exhibit 4001. I located the corresponding file within Trial Exhibit 4001 and reviewed its contents in both graphical and text-based readers. I verified that Halliburton Exhibit 4 appears to me to be an accurate rendering of the contents of file “uce.2016042418.028286.eml” from Trial Exhibit 4001. I then reviewed Halliburton Exhibits 5 and 6 and confirmed that they also appear to me to be accurate renderings of the email attachments included within the file “uce.2016042418.028286.eml.”

24. I reviewed Halliburton Exhibit 7, which was represented to me as a graphical rendering of the contents of the file “uce.2015111012.020599.eml” from Trial Exhibit 4001. I located the corresponding file within Trial Exhibit 4001 and again reviewed its contents in both graphical and text-based readers. I verified that Halliburton Exhibit 7 appears to me to be an accurate rendering of the contents of the file “uce.2015111012.020599.eml” from Trial Exhibit 4001. I then reviewed Halliburton Exhibit 8 and 9 and verified that they also appear to me to be accurate renderings of two of the numerous email attachments included within the file “uce.2015111012.020599.eml.”

25. I reviewed Halliburton Exhibit 10, which was represented to me as a graphical rendering of the contents of the file “uce.2013070803.011501” from Trial Exhibit 4001. I located the corresponding file within Trial Exhibit 4001 and reviewed its contents in both graphical and text-based readers. I verified that Halliburton Exhibit 4 appears to me to be an accurate rendering of the contents of file “uce.2013070803.011501” from Trial Exhibit 4001.

C. <u>The files “uce.2016042418.028286.eml” and “uce.2015111012.020599.eml” from Trial Exhibit 4001 contain emails and/or attachments that appear unrelated to [redacted] (Corporate Victim #2) or [redacted] (Corporate Victim #1).</u>

26. I identified the file “uce.2016042418.028286.eml” from Trial Exhibit 4001 in a folder named “[redacted].2-14 IP Range\[redacted].6”. The file contains two email attachments,

only one of which is associated with the IP address [redacted].6, which, as described above, is operated by [redacted] and has been since at least February 24, 2012. The IP address is associated with the domain name [redacted].com.br and is not overtly associated with [redacted] [redacted] (Corporate Victim #2) or [redacted] (Corporate Victim #1). The second email attachment within the file “uce.2016042418.028286.eml” does not contain any content, IP addresses, or domain names readily identifiable as being associated with [redacted] (Corporate Victim #2), [redacted] (Corporate Victim #1), [redacted], or [redacted].com.br.

27. I identified the file “uce.2015111012.020599.eml” from Trial Exhibit 4001 within the folder “[redacted].2-14 IP Range\[redacted].8” and a copy of the same file within the folder “[redacted].2-14 IP Range (No Duplicates)\[redacted].8”. The file contains more than 30 email attachments, only one of which is associated with the IP address [redacted].8. The remaining email attachments do not appear to me to contain any content, IP addresses, or domain names readily identifiable as being associated with [redacted] (Corporate Victim #2), [redacted] [redacted] (Corporate Victim #1), [redacted], or [redacted].com.br.

D. **<u>The file “uce.2013070803.011501” contains an email submitted to the FTC by an automated software program.</u>**

28. I reviewed the contents of the file named “uce.2013070803.011501” contained within the compressed archive “Batch Search Results.zip” from Trial Exhibit 4001. The file appears to represent an email sent from the email address “postmaster@[redacted]” to “abuse@namecheap.com”, with copies to itself, “spam@uce.gov”, and “support@namecheap.com.” The contents of the email include the following text:

```
ACTION
Removal instructions for 'spammed domains' are in this link:
        http://www.spamtrackers.eu/wiki/index.php?title=Registrar_Advice

Once removed with that method, this Complaint Generator tool
```

```
will create no more requests on this domain.
```

29. In my opinion, the text above suggests that the email was sent to the recipients—including “spam@uce.gov”—by an automated software program (i.e. the “Complaint Generator tool”) rather than by an individual. Additionally, the reserved mailbox name “postmaster” within an email address (e.g. “postmaster@[redacted]”) is a special address typically used by email server software to send or receive errors or other notifications from other email servers,[3] and is not typically associated with an individual email user.

October 20, 2016

Dr. Matthew J. Edman

[3] See, for example, RFC 5321 “Simple Mail Transfer Protocol” Section 2.3.5 (https://tools.ietf.org/html/rfc5321)